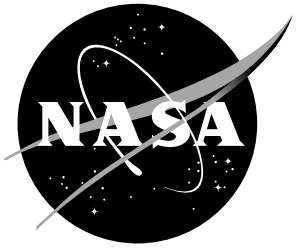
NASA/TM–2016–219446



Workshop on Assurance for Autonomous Systems for Aviation

(Guillaume Brat)
(NASA Ames Research Center)

(Misty Davies)
(NASA Ames Research Center)
(Dimitra Giannakopoulou)
(NASA Ames Research Center)
(Natasha Neogi)
(NASA Langley Research Center)

May 2016

NASA STI Program. . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI Program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI Program provides access to the NASA Aeronautics and Space Database and its public interface, the NASA Technical Report Server, thus providing one of the largest collection of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

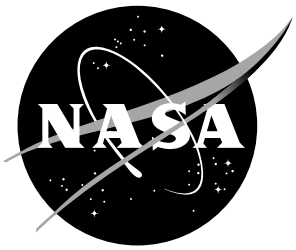
- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers, but having less stringent limitations on manuscript length and extent of graphic presentations.
- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.
- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.
- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.
- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.
- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include organizing and publishing research results, distributing specialized research announcements and feeds, providing information desk and personal search support, and enabling data exchange services.

For more information about the NASA STI Program, see the following:

- Access the NASA STI program home page at `http://www.sti.nasa.gov`
- E-mail your question to `help@sti.nasa.gov`
- Phone the NASA STI Information Desk at 757-864-9658
- Write to:
  NASA STI Information Desk
  Mail Stop 148
  NASA Langley Research Center
  Hampton, VA 23681-2199

NASA/TM–2016–219446



Workshop on Assurance for Autonomous Systems for Aviation

(Guillaume Brat)
(NASA Ames Research Center)

(Misty Davies)
(NASA Ames Research Center)
(Dimitra Giannakopoulou)
(NASA Ames Research Center)
(Natasha Neogi)
(NASA Langley Research Center)

National Aeronautics and
Space Administration

Ames Research Center
Moffett Field, California 94035

May 2016

Available from:

NASA STI Program / Mail Stop 148
NASA Langley Research Center
Hampton, VA 23681-2199
Fax: 757-864-6500

Abstract

This report describes the workshop on Assurance for Autonomous Systems for Aviation that was held in January 2016 in conjunction with the SciTech 2016 conference held in San Diego, CA. The workshop explored issues related to assurance for autonomous systems and also the idea of trust in these systems. Specifically, we focused on discussing current practices for assurance of autonomy, identifying barriers specific to autonomy as related to assurance as well as operational scenarios demonstrating the need to address the barriers. Furthermore, attention was given to identifying verification techniques that may be applicable to autonomy, as well as discussing new research directions needed to address barriers, thereby involving potential shifts in current practices.

1 Introduction

In the near future, autonomy will play an important role in civil aviation, and its applications will encompass a wide range of vehicles and platforms (e.g., from small UAVs up to transport-class aircraft, from low speed to supersonic and hypersonic aircraft etc.) as well as airspace operations, and vehicle health management systems. This infusion of autonomy is driven by a need to optimize airspace operations in order to accommodate increasing traffic density (e.g., adaptive trajectory-based operations, autonomous tugs, close parallel runways, and dynamic separation assurance), reduce operational costs to ensure that US operators can compete with emergent countries, and enable new business models (e.g., fire fighting, UAS-based package delivery, and precision aerial photography). In essence, virtually every component of the National Airspace System will become increasingly autonomous. Yet we need to enable this transition in a safe manner, and have techniques and processes in place to ensure the safety of the public.

Autonomous systems are characterized by their ability to make and execute decisions with reduced or no human intervention and by attributes such as self-configuration, self-optimization, self-protection and self-healing. These systems present new assurance challenges, and raise the following questions:

- **Can current assurance methods address autonomy?** Where are the limits to current techniques and how can we go beyond them? Should we limit the degree of autonomy when considering safety?
- **Do we really need to sacrifice performance for assurance?** Can we drive towards a notion of performance-based assurance?
- **How can we reason about human interaction with autonomous systems**, especially when the autonomous system hands over control to the human?
- **How do we provide assurance for existing systems**, especially when they were not originally developed to the required design assurance levels?

- **Can we address assurance challenges in less time than it takes today?** Can it be done without requiring a high-level of analytical skill on the part of the practitioner?

The purpose of this workshop was to identify where the current state-of-the-art lies in assuring increasingly autonomous systems, along with what research gaps exist, as well as how NASA can work with all stakeholders to provide assurance techniques that preserve the performance benefits of autonomy. The workshop included participants who represent industry (manufacturers, retailers, services delivery operators, air transportation experts, system designers and integrators), academia, government organizations, and subject matter experts. Collaboration opportunities were discussed towards aiding in the development and demonstration of assurance techniques for increasingly autonomous systems.

The workshop was co-located with the SciTech 2016 conference in San Diego, CA. It ran for two days, and encompassed for a total of four sessions:

- Wednesday 9am to 12:30pm: Describing Autonomy for System Assurance: panel, lightning fast talks, and discussion.
- Wednesday 2pm to 5:30pm: Methods for Enabling Autonomy: talks by John Valasek (Texas A&M, Director of the Center for Autonomous Vehicles and Sensor Systems) and Eric Johnson (Georgia Tech, Lockheed Martin Associate) Professor of Avionics Integration), followed by a break-out session.
- Thursday 9am to 12:00pm: Managing Key Issues for Assured Autonomy: talk by Steven Young (NASA Langley Research Center), panel, and lightning fast talks.
- Thursday 2pm to 5:30pm: Assurance Tools and Techniques for Trusted Autonomy: panel, wrap up.

The following section summarizes our key findings while subsequent sections provide more details about each session. The appendix lists the participants of the workshop. Some people attended only a subset of the sessions. While reading the rest of the report, the reader should keep in mind that we organized and focused the workshop around the following points:

- Discussion of current practices for assurance of autonomy.
- Identification of barriers specific to autonomy as related to assurance, as well as operational scenarios demonstrating the need to address these barriers.
- Identification of verification techniques that may be applicable to autonomy.
- Discussion of new research directions needed to address barriers, potentially involving shifts in current practices.

2 Key Findings

In this section we present some of the key findings from the workshop. This section serves as a summary of prioritized points, selected by the workshop organizers, and is by no means comprehensive. A detailed reading of the session particulars is encouraged so that an informed and unbiased view can be drawn, and further insights gained. Furthermore, the session transcripts can provide an archival source of information regarding the topics and participation engendered by the workshop.

First among the gathered points is:

> Verify not what system will do, but what system must not do.

This was a recurrent theme of the workshop. Existing V&V processes are focused on what the system does, and whether it does so safely. The participants felt that there needs to be a paradigm shift for autonomous systems. Given how much is unknown about the system during the design and development stages of the life cycle, many participants argued that V&V efforts should focus on ensuring that the system does not exhibit incorrect or unsafe behaviors at runtime.

> Incorporate probabilistic reasoning techniques, especially into models for V&V.

There is a need for advanced probabilistic reasoning support in V&V techniques, (both spatial and temporal) for autonomous systems. There is a special need for inferring models from data. Several presenters pointed out that formal methods lack adequate support for reasoning probabilistically about autonomous systems, especially since such systems can exhibit stochastic or non-deterministic behavior (e.g., uncertainties in the operating environment, complex interactions between computational elements or environment, etc.).

> Identify ramifications of a possible shift from certifying systems to licensing systems (as for cars)?

The issue of licensing autonomous systems rather than certifying them came up several times. Many participants drew a parallel between the certification of these increasingly autonomous systems to that of humans driving cars: Humans are trained and tested in order to obtain licenses for driving (operating) within the transportation system. Licensing is a standardized process and as such, it can improve driving quality and the handling of exceptional situations. This is an issue that is very germane to the notion of trust.

Provide new V&V methods for learning and adaptive systems.

One of the new features of autonomous systems is their focus on learning on-the-fly; these systems may also learn off-line. The ability of a system to learn is not addressed adequately by current certification standards. This topic is related to the issue of detecting undesirable behavior in the sense that we would wish to verify that the system does not learn incorrect or improper information, if we could determine what such information is.

Provide new V&V methods for model-based software systems.

The use of model-based software development results in non-traditional software, in which the rationale/logic is not necessarily reflected in the code (or the structure of the code) but more in the models that are used to generate the code or that are consulted at run-time. This presents new challenges that could be addressed through testing, but at a high cost. Therefore one needs better and cheaper V&V methods focused at the model level

Human-machine teaming issues are a barrier to autonomy assurance.

Human Machine teaming issues were identified as the largest barrier to developing standards for certifying increasingly autonomous systems. In general, there is a consensus that autonomy on its own is hard to assure but is even harder when it interacts with humans to accomplish a common goal.

Further complicating this issue is the fact that there is a need to understand how to achieve high levels of assurance without the human functioning in a traditional safety critical role. It has long been argued that it is unknown what the exact contribution to safety the human really has. Further investigation into this topic is required in order to properly assure autonomous systems.

Cyber-security can no longer be ignored in autonomous systems.

Cyber-security has been identified as a major concern for autonomous systems. However, the role it will play in assurance, and the weight that it will be given with respect to autonomous system safety, are still under debate. The full range of assurance implications arising from cybersecurity issues is not yet understood. However, it is unclear if cybersecurity concerns should explicitly be a part of certification standards for autonomous systems, or whether there exists an alternate means by which they can be addressed.

Study and draw from other fields currently employing autonomy, such as the automotive and robotics industry.

The automotive industry has been cited as an example for the deployment of autonomous systems. Some participants also brought up experiences with robots, especially observing their behaviors during grand challenge competitions. There is a consensus that we can learn from the experience garnered in these industries when it comes to issues such as trust, understanding (which is related to trust), and assurance.

3 Session 1: Describing Autonomy for System Assurance

In this session, we aimed at surveying the state-of-the-art in assurance of autonomous systems, as well as current practices used to achieve assured autonomy. Topics that were addressed include a discussion of this years Workshop on Certification of Non-Deterministic Systems, the recent NRC report on Autonomy Research for Civil Aviation, along with discourse on current practices in the UAS industry as well as at NASAs Autonomy Incubator.

We began with a panel discussion to explore these areas, via an interactive Q&A session with the audience. This was followed by several lightning-fast (5 minutes) talks on new ideas for describing and generating requirements for autonomous systems. Here follows a short summary of the session.

- Goals: Identify key requirements for autonomous systems that have critical safety constraints
- Panel:
  - Danette Allen (NASA Langley)
  - Ella Atkins (University of Michigan)
  - Andrew Lacher (MITRE)
  - Lael Rudd (Lockheed Martin Advanced Technology Laboratories)
  - Andy Thurling (AeroVironment)
- Audience: 70
- Strengths
  - Industry perspective well represented
- Ideas (connective, knowledge sharing)
  - Verify not what system will do, but what system will not do
  - User sophistication is an influence/direct factor in the degree of autonomy

- Examples
  - Science missions
    - natural interface, resistant to environment, object detection and classification, avoidance, obstacle under tree canopy
  - Precision agriculture
  - Solar-powered, high-altitude UAVs for internet
  - Geofencing as a V&V/C case study
- Challenges
  - UAVs
    - Unpredictability of these complex systems makes them hard to understand and thus trust
    - Also, lots of non-determinism in environment
  - V&V
    - Need more exhaustiveness than in testing
    - Need to also verify interactions with humans (Theory of Mind)
    - Prove that system will not do bad things
    - Use runtime monitoring and then go to run-time assurance
  - Certification
    - Is licensing a good model? Demonstrate proficiency to generate trust
    - Airworthiness vs. operational certification (mission implies environment, which brings non-determinism)
    - Paradigm shift: certify that autonomous systems cannot do bad things
    - Might end up being driven by accountability and liability

3.1 Panel

This section presents our notes (not everything has been captured) on each of the panelists presentations.

Danette Allen (NASA Langley)

Danette Allen runs the Autonomy Incubator at NASA Langley where her research team experiments with robotic and aerial autonomous systems. Some of the main points in her presentation were as follows: UAVs are systems and should be designed as such from the start. The community needs more and better facilities/testbeds to evaluate UAVs and accumulate data to drive our assurance requirements. For her work, all COAs are obtained based on the presence of a backup remote pilot. She also highlighted the following two challenges: (1) Systems cannot learn by analogy - as a consequence, autonomous systems can be very fragile and

break often especially when something new and similar but not identical is encountered. It is important to make them more robust. (2) V&V for autonomy needs to be more exhaustive than just testing.

Andy Thurling (AeroVironment)

Andrew J. Andy Thurling is a former test pilot for the Air Force and is now the Director of Product Safety and Mission Assurance at AeroVironment in Simi Valley, California. Some of the main points in his presentation were as follows: The word Autonomy scares regulators, probably because of a lack of trust due to the associated uncertainties. We should start with easy cases, e.g., precision agriculture (well-known, confined environment) and solar-powered, high-altitude UAVs for internet, and then work our way up to more challenging operations, e.g., package delivery. Trust comes from knowing that the system will not misbehave.

His talk raised the comment that, when it comes to assurance, it boils down to accountability and therefore this will drive regulation.

Lael Rudd (Lockheed Martin)

Lael Rudd works in the Intelligent Robotics Laboratory at Lockheed Martin Advanced Technology Laboratories and provides support for autonomy programs at Lockheed Martin. Here are some the main points in his talk: For manned/unmanned teaming one needs the ability to incorporate the mental state of human systems and the mental state of autonomous system. He is currently working on methods based on the Theory of Mind. He also made the point that we should really separate mission goals from decision-making, which is where the safety issues really are. In autonomy, he sees the following open challenges: The role of humans in collaboration with autonomy must be studied and analyzed. Theory of mind and belief logic were discussed as framework possibilities. It is important to be able to link cognitive and machine theories in a unified analysis framework. There is a lack of good, reliable data; we also need good metrics. He proposes that the highest priorities should be as follows:

- Understanding the behavior of adaptive/non-deterministic systems.
- Designing autonomous systems that operate without continuous oversight.
- Modeling and simulation, V&V and certification.

His talk brought the comment that goodness-of-fit is underlying the current regulations. Lael Rudd agreed but he remarked that it is not the way people think about it and it also does not catch the in-between. This brought up a discussion about licensing, which demonstrates proficiency. This is the first time, but not the last, when licensing was brought up as an alternative to certification for autonomy.

Andrew Lacher (MITRE)

Andrew Lacher works at MITRE, at which he has a leadership role in defining the MITRE Corporations research strategy in unmanned and autonomous systems. Andrew gave a summary of the workshop on certification of non-deterministic systems held at MITRE, MacLean VA, in November 2016. The workshop brought the certifiers to talk with the researchers and some of the main findings were as follows:

- The sources of non-determinism in autonomous systems are inputs, probabilistic algorithms, adaptive/learning systems, and COTS.
- Autonomy example for certification: PrecisionHawk (a pilotless agricultural UAV) in which a farmer can pick goals, but does not fly the UAV.
- FAA already has a sliding scale for safety (GA aircraft to transport aircraft), which could be adapted for autonomy.
- We should change the certification paradigm and certify what the system will not do because it is impossible to evaluate all conditions before deployment.
- Plausible architecture for facilitating assurance: deterministic modules can be responsible for safety and the system can include the notion of safety nets.

Ensuing discussions to Andrew Lachers talk showed that there is a split in the audience between certifying for airworthiness and certifying for use in missions. Somebody also questioned that a human pilot can be seen as non-deterministic, so why require deterministic modules for safety. The response was that no humans are deterministic, but pilots are licensed (but not certified), which brought up again a discussion about licensing, trust, and proficiency. Some questioned why the human is put on a pedestal and not autonomy when there are autonomous safety systems such as electronic geo-fencing (GF) (e.g., keep-out GF and keep-in GF).

3.2 Lightning Fast talks

We summarize very briefly the main points developed in 5-minute talks.

Devesh Bhatt (Honeywell Aerospace Labs)

Devesh Bhatt stated that humans are bad at monitoring. Automation should work as a colleague. We need an automation paradigm shift to enable single-pilot operations. Still all verification must be done with respect to requirements; therefore we need good autonomy requirements.

Corey Ippolito (NASA Ames Research Center)

The UAV community seems to move away from the aviation community (which echoed some earlier comments that IT companies are pushing the issue for UAVs rather than the traditional aerospace companies). Corey Ippolito also presented the UTM project developed at NASA to provide air traffic capabilities for UAVs.

Greg Dorais (NASA Ames Research Center)

Greg Dorais asked what the difference is between automation and autonomy (is it self-governing?). For him, autonomy encompasses the ability to manage risks: It can identify a risk, manage it, and learn from its mistakes. That could be a key to demonstrating the ability to reach proficiency, as is done when we license humans for driving cars.

Tom Apker (Naval Research Laboratory)

Tom Apker is building a run-time monitoring system that provides an LTL-based safety cage around autonomy. When the system is about to leave the cage, one can implement safety measures. The work is using game theory to come up with the controller and it can help prove that the system cannot go into unsafe situations.

Yu Gu (West Virginia University)

Yu Gu presented an analogy from the robotics world. In a robotic challenge, he could not understand what the other robots were doing, which led him to state that it is hard to predict the behavior of an autonomous system. Moreover, as he said, if you do not understand something how can you trust it? He also questioned even attempting the idea of assured autonomy in unstructured environments.

Florian Adolf (DLR: German Aerospace Center)

Florian Adolf thinks that we need basic requirements for trustworthiness. Perhaps we should build on the traditional robotic three basic rules: do no harm, obey, and protect yourself. For aviation it could be: do no harm to living being (air or ground), do no harm to other UAVs, do no harm to other objects

3.3 Discussion

The session ended with a spirited discussion about the following points:

- Autonomous systems do have minds; these minds are not easy to understand, but they exist. To this point, somebody added that unpredictability is the key factor as shown by the robotic experience described earlier.
- The analogy to driving licenses was the next topic. Somebody brought up the time to learn (16/18 years old) but the point was made that AI could do it faster. This was not resolved as shown by the last remark that there is an age to trust ability to mitigate risk and we do not know what this age correlation is for AI.
- At this point, it was brought up that autonomy does not mean strong artificial intelligence (AI). Somebody remarked that the problem with weak AI is that

you have to build learning in rules, which led to the response that it is not true and weak AI can learn.

- The last discussion point was about certification. Perhaps shooting for full certification is wrong. Maybe we just need to certify the health monitoring system. There was broad agreement on having an envelope that prevents you from becoming unsafe; the idea of runtime assurance came back several times. It does not solve everything: how do you assure that you go into a true safe state? It was then suggested that it could be demonstrated on easier missions first. The final comment was that mitigation is a second step. We should first focus on monitoring; it is the first problem to solve.

- The statement was made that the more intelligent a system, the safer it is. On the other hand, another statement was made that increasing system sophistication increased its vulnerabilities. Cyber-security was brought up at this point too.

- Regulation is still a major issue. Even for simple missions that involve agriculture, it is extremely hard to obtain permission to fly them. There must be a pilot on the ground for each autonomous vehicle so that they can take over if needed. Often, drones must be tethered to obtain permission. The regulatory aspect does not seem to be easily addressable at the moment.

4 Session 2: Methods for Enabling Autonomy

In this session, we discussed current and upcoming techniques that are driving autonomous system development in aviation and the need for new assurance techniques in order to enable greater assured functionality for autonomous systems. The initial list of topics of interest included the design, manufacture, fielding, maintenance and retirement of autonomous systems, including relevant elements such as COA/Certification and regulatory approval. Architectures for autonomy were also discussed. Presentations and discussions addressed mostly the design and fielding of autonomous systems and what has been done, or need to be done, to obtain regulatory approval.

We began this session with subject matter expert presentations, addressing the issues inherent in designing and fielding multiple types of autonomous platforms with differing mission capabilities and assurance levels. We then formed moderated breakout groups to explore the themes of human-machine teaming, trust in autonomy, and V&V challenges for complex/adaptive/learning systems.

4.1 Talks

John Valasek (Texas A&M University)

John Valasek described the effort his group at Texas A&M takes to design UAVs and to evaluate their performance in the field. He touched briefly on what was

needed to obtain CoAs to fly these UAVs at a facility in a sparsely populated area. He also mentioned that they operated at or slightly above class G airspace, which made life easier in terms of regulatory approval. Here are some of his main points.

All his UAVs have a risk management process layer, which has been inspired by processes used in the NAS and at Boeing. UAS pilot certification has not been a problem at all. However, since the work is funded by and targeted at Air Force operations, they had to go through a series of USAF review boards. Overall they always perform a deep fault analysis for even the simplest functions.

The intelligent part of his UAS resides in the Intelligent Supervisor/Decision Support Tool. It performs hyper-trapezoidal fuzzy logic model inference. In general, they have tried to put the intelligence in the outer loops, which makes assurance an unconventional problem. John Valasek also mentioned that they were never given a hard time about the non-conventional part of their control system. Learning or adaptation were not on the minds of the USAF review boards they went through.

Eric Johnson (Georgia Tech)

Eric Johnson presented two cases studies of UAVs trying to address specific grand challenges for autonomy.

His first case study consists of a UAV helicopter having to find a building (marked with a specific sign), find an opening to enter (it took 3 or 4 attempts to find it), go inside and read some display (they had no success in entering the building through a window). Their design philosophy relies on a pyramid of maturity. In essence they keep building on top of elements with greater (or at least equal-level) maturity. It allows them to define a maturity scale for their research in a way similar to the TRL scale. Their adaptive control system was amongst the most mature of their components. They drew two big lessons from this challenge. First, use simpler components, and second, these systems are still too complex to ever be fully tested in real life.

His second case study consists of finding and driving an evader to a specific location for capture. Two unmanned aircraft collaborate to accomplish this. This mission has aspects of collision avoidance, terrain avoidance, and collaborative search. The main lesson they drew from this challenge was to use daisy-chained operators so that each of them can control N aircraft. The regulators for this challenge knew there was an adaptive controller but it did not attract additional scrutiny. John Valasek added that they had the same situation and the fact that humans had the ability to take control manually was enough to ease the concerns of the challenge regulators.

4.2 Breakout sessions

There were three breakout sessions with the following themes:

- Technology Transition and Establishing Trust.
- Human-Machine Teaming.
- V&V challenges for complex/adaptive/learning systems.

4.2.1 Human-Machine Teaming

Participants:

- Kerianne Gross, AFRL (chair)
- Devesh Bhatt, Honeywell Aerospace Labs
- Randy Bailey, NASA Langley
- Hai Yang Chao, University of Kansas
- Andy Thurling, AeroVironment
- Chris Thames, NASA Langley
- Lael Rudd, Lockheed Martin
- Misty Davies, NASA Ames
- Shu-Chieh Wu, NASA Ames (scribe)
- Lee Pike, Galois Inc
- David Bridges, Texas A&M

The breakout session was organized around several challenges: communication, V&V, and security.

Communication: One of the biggest challenges is the understanding of mutual behaviors and intent. How can you be sure that there are not mismatches?

A question was asked as to whether there were examples of good teaming. It seems to be hard to achieve a good balance. If the autonomy is too good, it leads to over-reliance by the people. If the autonomy is not good enough, it leads to a lack of trust in the autonomy by the people.

A core assumption by the group was that humans will be involved in the process in some role. It is important not to preclude the operator from getting control back from the system.

There was consensus in the group that we need to better understand teams of humans in order to apply the best practices to human-machine teaming. Cockpit communication has a particular cadence for example, which yields trust. It is important for expectations to be based on prior interactions.

We need research on what measurements need to be taken from the human so that the autonomy understands state and intent of the human.

V&V: In order to understand and improve V&V approaches, we need to try multiple V&V approaches for the same problems. We never get to do this.

Where are the National V&V centers? How can we get the necessary data? (systems, requirements, etc.) How do we account for the human contribution (e.g., measurements etc.) when we are doing V&V of human-machine systems? How do we measure the software? Is there a way to compare those V&V measurements when we do V&V at the system level?

There is a tendency to assess the human part of the system with probabilistic approaches, and the software part of the system with absolutes.

To what extent will the right human-machine teaming happen naturally if we allow the system to evolve? Is it even possible to smoothly evolve or are there dangerous and safe islands?

How do we do validation? How do we make sure that the automation is appropriate and transparent for the mission? How much information needs to be shared between the automation and people depends on the mission.

We need an equivalent of the Cooper-Harper rating for the mix of human and machine.

Security: When it comes to security, many of the issues are societal; for example, basic privacy principles must be respected when evaluating pilots. In general, humans and automation pose very different security risks. Humans are not secure systems. However, humans are less likely to fall prey to denial-of-service attacks.

General Points: More general discussion then followed on several aspects of human machine teaming. Topics included how to take into account workload in order to efficiently perform division of labor, how we can ensure safe transitioning of control, whether we could create classes of missions with similar human-machine teaming needs so that we can apply similar teaming and V&V strategies, and how V&V could incorporate issues of workload and degree of human engagement in order to properly assess the safety of a mission.

4.2.2 Technology Transition and Establishing Trust

Participants:

- Natesh Manikoth, FAA (chair)
- Andrew Lacher (MITRE)
- Natalia Alexandrov (NASA Langley)
- Jim Murphy (NASA Ames)
- Ben Di Vito (NASA Langley)

- Guillaume Brat (NASA Ames)

The breakout session started with preliminary discussion about the current certification process and the place of trust in the current system. Here are some of the main points that were discussed:

- This breakout session started with a quick reminder of the current airworthiness certification processes, especially for software since software is often at the core of an autonomy solution. Current process relies on the application of DO-178C, which is a process that promotes quality and rigor (and thus, generate trust through these attributes) rather than generating hard evidences for safety. It is also worthy to note that the current process trusts the development actors since checking DO-178C often resides in the hands of DER (Designated Engineering Representatives) who are employed by the company developing the product and not the FAA.

- Now, this trust is well placed because the air travel is very safe. In fact it would be very hard to make it safer than it is today. Yet as we go through the transition of allowing autonomous systems in our air space, the public expects that safety will remain at current level or improve if possible. In the eyes of the public, safety has to be an increasing monotonic function.

- The group then discussed the various reasons for introducing more autonomy, starting with the push for reducing crew. The cargo industry would obviously benefit from such a reduction and could be an early adopter since they are not carrying passengers, hence the safety requirements are less. On the other hand, airlines could also benefit from more autonomy as they always strive to reduce their operating cost. In both cases, we need to start with taking a closer look at the role humans play with regards to safety and why the public feels more safe with a human in charge. By the way, it shows that trust is relative to roles; we could probably accept more readily autonomous cabin service rather than pilot replacement with autonomy.

- Now there is another dimension to consider. The trust of the public in an airline is highly dependent on the airline service history. However, the trust placed by the FAA in the airlines are probably more dependent on the certification of their operating processes, e.g., crew training, maintenance, and so on.

- Then the group moved to the new actors in aviation such as the companies pushing autonomous package delivery or other new business models involving heavy use of drones. These systems are being perceived as non deterministic, even though the source of non determinism is probably coming from the environment. In any case, UAVs are seen as relying on new technologies like adaptive control or some kind of learning. This is a new technology that requires new certification processes.

This last point was a good segue for the group to move to the second part of the session and focus on the challenges ahead:

- Going deeper into the role humans play with regard to safety, the group advocating taking a closer look at the decision making process especially when it shifts from humans to machines. In that respect the interface between air traffic controllers and pilots is also of great importance as the potential for ambiguities is always present. We need to separate the function being performed (and its contribution to safety) and the current way its being realized; this should inform us as to whether it is advisable to replace humans by machines. As we mention before, safety and trust are relative to roles.

- Now it also led us to examine the notions of accountability and liability and the roles they play in trust. The general feeling is that if you can be made accountable or liable for accidents and their consequences, then you are more likely to pay attention to safety. If the function is done by a machine who becomes accountable? The airlines or the autonomy developer? The bottom line is that accountability and liability are key levers in air transportation safety.

- On the side of the new concerns with regard to autonomy is security. How do we ensure that malicious actors are not in control? Safety and security go hand in hand and should not be separated anymore.

- Lastly, a huge concern is that commercial development is faster than certification, both in coming up with new certification processes and going through certification processes. This was already a problem with the current systems, and, it will be even more of a concern with the influx of new industry actors, which are accustomed to fast moving markets. Note that commercial development can also outpaced the ability to generate trust. Service histories will be shorter and technology will involve faster that we can build trust for it.

4.2.3 V&V Challenges for Complex/Adaptive/Learning Systems

Participants:

- Dimitra Giannakopoulou (scribe)
- Florian Adolf, DLR
- Robert Moore, Embry Riddle
- Thomas Apker, Naval Research Laboratories
- Christopher Torens, DLR
- Sangeeth Ponnusami, Airbus
- Joerg Dittrich, DLR
- Zohaib Mian, United Technologies Research Center
- Shankar Natarajan, SRI

- Greg Dorais, NASA Ames
- Yu Gu, West Virginia University
- Natasha Neogi, NASA Langley

The first part of this break-out session focused on having each participant identify the one characteristic of complex/adaptive/learning systems that is the most challenging and pressing to address. The list of characteristics is provided below.

- Autonomous systems must monitor their environment and must make interpretations about it.
  - Also, how do we classify noisy sensor data?
  - How do they do learning from that? Current autonomous systems cannot learn by analogy.
- There are needs for
  - determining what are the actual requirements.
  - identifying and stating explicitly assumptions between different components for adequate integration.
  - defining how to test adaptation and how to identify scenarios that endure that adaptation is appropriate in all important cases?
  - identifying an adequate notion of test coverage for such systems.
  - defining new methods to evaluate quality of systems that deal with uncertainty: what is good enough and where is the bar?
  - defining proper failure modes.
    - How can we take into account all the problems that can occur and test if the system reacts appropriately without making the cost of testing prohibitively expensive?
  - achieving architectural simplicity and modularity, leading to decoupling the analysis of the different parts of the system, with potentially different strategies for components with different characteristics (e.g. adaptive components vs. more traditional ones).
    - Scalability is also an issue.
  - defining a new certification standard so that one can gain certification credit for theoretical proofs, and incorporate alternative techniques for achieving certification.

The question posed in the second part of the session was whether existing technologies could be used or extended towards the V&V of such systems, or whether fundamentally new and different approaches are needed. The topics discussed are listed below.

- Assurance

  - We need to come up with metrics of safety for learning (as opposed to non-learning) systems.

- Requirement aspects
  - Identification of requirements specific to these types of systems is needed to enable the application of V&V techniques.
  - We also need to develop techniques for transforming natural language requirements into formal ones.
  - Requirements must be considered as tests for the system to pass; in general, we need to rethink the process associated with requirements and provide education for better writing of requirements and associated tests.

- V&V aspects
  - Formal methods must be implemented in a scalable fashion potentially with contract-based design.
  - There is a lack of high-fidelity physical models - having them would make the development of adaptive systems much better.
  - There is a need for probabilistic reasoning (both spatial and temporal) and inferring models from data.
  - There is a need for developing hybrid (as opposed to software only) solutions that combine digital and analog/physical systems.
  - Methods to determine the level of verification that should happen off-line and the residual risk being dealt online and at runtime.

- Design
  - Novel formalisms and methods are needed to address the characteristics that are specific to adaptive systems.
  - We must develop novel architectural approaches; knowledge-based architecture was brought up as an example, where rules describe how a system evolves.
  - We also need design support tools to mitigate the risk and development cost, e.g., maybe aircraft that does not harm anyone if it crashes?

5 Session 3: Managing Key Issues for Assured Autonomy

In this session, we examined several key challenges that directly impact our ability to generate assurance arguments for increasingly autonomous systems. Topics that were addressed include human-machine interaction in the context of increasingly autonomous systems, the management of uncertainty, and the management and mitigation of communications criticality.

We began with a talk exploring the effects of human-machine teaming on autonomous systems, followed by a panel about uncertainty management and mitigating the effects of communications criticality. We finished with a set of lightning-fast (5-minute) talks for all assurance of autonomy themes.

- Goals: What aspects that are unique to autonomy also make it difficult to assure (both safety and certification)? Can you give concrete examples for each aspect?
- SME talk: Steve Young (NASA Langley)
- Panel: Steve Young (NASA Langley), Kerianne Gross (AFRL), Jim Murphy (NASA Ames), Natalia Alexandrov (NASA Langley), Mats Heimdahl (University of Minnesota)
- Panel Audience: 50/40 approx
- Strengths
  - Lightning talks encouraged participation from audience members who had not previously provided input (non-traditional participants)

Summary of ideas discussed:

- Need to understand how we achieve high levels of assurance without human functioning in traditional safety critical role
- Automotive industry cited as an example for deployment of autonomous systems
- More call for certifying what should not happen.
- More proposals to go to runtime monitoring and assurance.
- More calls to look at role of humans.
- More calls for more data and being open.
- More thinking that liability and accountability will drive the standards. Regulation may eventually come from the legal system.
- Calls for:
  - model validation.
  - use for compositional verification for fighting complexity.
  - local control.
  - cybersecurity.
  - architecture with trusted, deterministic layers.
  - cost models.

- Acknowledgement that current methods are not sufficient.

General Observation: The current approach to safety is that we constrain the behavior space in order to get away with not being able to predict all possible outcomes. For example, to constrain the airspace we use procedures, remain within visual line of sight etc. A potential new approach to V&V would be to set the constraints very broadly and learn as we fly, and thus improve integrity over time. Another approach, assuming that we are not able to fully verify autonomy, is to introduce protective measures. Geo-fencing, a popular example, tries to restrict the operational space of an autonomous mission. As another example, NASA Langley has developed a highly assured stand alone module that can be attached to a UAV, which monitors and predicts for non-conforming behavior (see sub-section on the talk of Steve Young). Thus, a potential approach to V&V would be to monitor novel algorithms at runtime, by having them shadow real flight data and see how they compare to actual pilot behavior.

5.1 Talk

Steve Young (NASA Langley)

Steve Young started by giving many examples of existing autonomous functions: ACAS, GCAS, interval spacing etc. He then followed with the statement that we have to think of how big systems (vehicles, environment, ATM) interact. Most of the time we can bound the performance of systems, including autonomous systems, and it helps in analyzing them.

Steve Young followed with a few remarks on the human contribution to safety, which was a topic raised the day before. He thinks that we should keep the human at least as a monitor and as an independent (for the system) observer. Yet he is not sure that we can truly quantify the human contribution to safety. For assurance we need to provide trusted information to the decision maker. He added that information integrity requires at least two independent sources. That led to some remarks on V&V, in which we should check our assumptions and allow for learning as we go. We should also record everything to get more data for deploying new systems.

For vehicles, Steve Young argued for the deployment of reliable autonomous safety-net technology, especially for unmanned system. This included ideas like run-time monitoring, assurance and certifying what should not happen (again a recurring theme in this workshop). Steve Young contrasted what the public demands with what industry demands. The public demands affordability, safety, security, and privacy. Industry tries to address public demand but it also wants to minimize liability.

Next Steve Young described an example, in which a small box can be attached to a UAV for monitoring for non-conformance, and inform the pilot (or auto-pilot) that the UAV is getting too close to constraints (similar to geo-fencing, but with assurance arguments). His solution does not rely only on GPS. Responding to questions from the audience, Steve Young said that

- the integrity of the localization system can be achieved by having two independent systems, which can use independent frequencies to avoid correlation, and,
- the problem of outdated information is already addressed in the newly updated database standards.

5.2 Panel Discussion

Natalia Alexandrov (NASA Langley)

Natalia Alexandrovs presentation revolved around the main idea that we will have to deal with a primordial soup of uncontrolled UAVs, with potentially uncooperative participants. There are two approaches we could take to dealing with this fact. (Case 1): to control, you have to have a tacit agreement that the participants want to be controlled (and regulated); of course, higher density of traffic might create a tractability problem. (Case 2): benign participants must change and be more survivable (e.g., design more maneuverable aircraft). Thus, we need a control architecture for cooperative participants and we need to design for controllability, robustness, resilience, and adaptability at all scales. There is also a need to manage contingencies for non-cooperative and malicious participants; conforming participants will need detection and protection capabilities. Natalia Alexandrov is in favor of local control (rather than a large centralized control system) and believes that we need better situational awareness and cybersecurity. She also argued for a tighter coupling of airspace design and aircraft design. Her conclusion is that we need complexity-bounded multi-scale self-organized decision making.

Kerianne Gross (Air Force Research Laboratories)

Kerianne Gross presented the point of view of the Air Force on autonomous systems. USAF sees autonomy as game changing. Human-machine teaming and interaction, as well as trust are seen as very important in this context. Therefore, AFRL studies the changes in human roles carefully.

She presented the example of the automated collision avoidance technology for the F16, which automatically maneuvers an F16 out of the way in case of a possible collision. Its requirements are: do no harm and do not interfere (which is the toughest for Air Force pilots). They have seen good pilot acceptance; in fact they see almost too much trust from the pilots. Their other big challenge is the integration of independently-developed autonomous systems, especially when it comes to V&V. They are investing in the use of modular/compositional V&V. They also wonder how to formalize autonomous system models so that we can do mathematical analysis. AFRL is doing a lot of physical testing to validate their models. Ideally the compositional framework would help in combining the evidence.

Jim Murphy (NASA Ames Research Center)

Jim Murphy is the main designer for the UAS in the NAS testbed at NASA. He therefore drew from his testbed experience to think about autonomy. He pointed out that the first thing to do is to understand the domain but that you almost always miss requirements. So, this needs to be taken into account in the design; it needs to be extensible. He is also a big proponent of open access (to gather feedback from the whole community) and data collection. He thinks that it is critical that everybody (including academia) can use these systems.

Mats Heimdahl (University of Minnesota)

Automation and tools are very useful, especially in V&V. There is a reluctance to use these tools (same as autonomy) because we do not have enough data. However, we are already in trouble: autonomy is coming and our old techniques are not applicable. For autonomy, it is more a validation problem than a verification problem: do we have the requirements right? We need to think more about system safety, rather than focusing on software. For autonomy, we need a sort of Turing test for driver. Regulations will come from the legal system: liability will drive these regulations. The actual problems will appear because of the participation of small players; big players have too much skin in the game, they have to be more careful. Assurance cases are touted as a possible resolution, but they are not going to be water-tight. We will need to rely on beliefs, and we need to know how to fold these beliefs into our analysis.

Further Discussion:

Some of the topics that were raised during the panel discussion include the following:

Can we ensure that software is trained for all situations that may occur? We do not have a good answer to this question yet, even though it is important. The audience and panelists discussed the issue of licensing, and it was mentioned that AFRL has a study on a licensing paradigm. The Toyota unintended acceleration problem was presented as an example of humans not understanding what the automation is doing.

When safety measures are introduced to ensure safe boundaries for a UAS, such as geo-fencing for example, one would still need to detect if the safety measure will fail. Finally, since in reality autonomous software is non-deterministic, what is the point of testing with deterministic inputs? We do not have good probabilistic evaluation methods, but we can use bounds as test oracles.

5.3 Lightning fast talks

Mark Skoog (NASA Armstrong) described his work on developing an expandable variable-autonomy architecture with run-time assurance. A safety case is developed to support it.

Joerg Dittrich (DLR) described their work on pilotless aircraft and made some good points by introducing data and statistics. He claimed that solutions to low reliability of UAS may not involve classical certification methods that may over-restrict the operations. Rather, approaches that avoid damage their surroundings may be more realistic. He brought as an example a German UAS equipped with a parachute that is deployed automatically if the UAS malfunctions and is to fall on the ground. He also argued that affordability of the verification techniques has to be a major driver given the fast rate at which UASs are introduced in the airspace/ The use of automated tools as well as benchmarks could contribute to affordability.

6 Session 4: Assurance Tools and Techniques for Trusted Autonomy

In this session, we explored new concepts and methods to facilitate the Verification and Validation (V&V) and Certification of increasingly autonomous systems. Topics that were addressed included tools and techniques that can be used to assess and assure safety and security. We also investigated tools and techniques that engender trust in increasingly autonomous systems on behalf of designers, evaluators, users and the general public.

- Goals: Does autonomy require a shift in assurance processes?
- Panel: Lee Pike (Galois), Natarajan Shankar (SRI), Cristoph Torens (DLR German Aerospace Center), Darren Cofer (Rockwell Collins), Irene Gregory (NASA Langley)
- Panel Audience: 30 approximately
- Strengths
- Expertise in V&V tools well represented on panel

Brief Summary:

Barriers to certification: Well defined requirements, Verifiable behavior, Predictable performance, No unintended functionality.

Are the problems that we discuss particular to autonomy or are they systems problems?

Architecture provides an opportunity for mitigating the assurance of autonomy. Examples include

- geo-fencing (spatial constraining),
- runtime monitoring (perform recovery actions when unanticipated problematic situations occur), and

- ability to turn adaptive behavior on or off (e.g., switching adaptive behavior off during abnormal conditions, or engaging adaptive behavior to recover on conditions where you would lose aircraft anyway).

The topic of licensing versus certifying was also discussed a lot in this session. It was explored further and brought up the following questions.

- How do we license humans?
- How do we trust humans to perform a job?
- Are our fears of autonomy unfounded?
- Do we really test humans that much more, or, we actually trust them without much evidence?

The other point being brought up many times is that we should only consider new algorithms if there is a clear benefit. For a safety-critical system, we should also show that they are safe. In principle we should be able to modify our processes to accommodate autonomy if the benefits are clear.

6.1 Panel

Lee Pike (Galois)

Lee Pike s main statement was that autonomous system challenges are just systems challenges. The real challenge resides in modeling the environment and its uncertainties. Therefore Lee Pike suggested that the community focuses on probabilistic techniques to approximate a correct environment, e.g., hidden Markov models. Lee Pike also thinks that we should try to characterize the types of requirements faced in autonomy and focus on behavioral bounding boxes.

Natarajan Shankar (SRI)

Natarajan Shankar claimed that the challenges presented by autonomy are not really new and that we have been dealing with them for a long time under the name of automation.

For him architecture is the key issue. One must design a system for assurance. The goal is the creation of an efficient argument (one that is easily refuted if it is wrong). He advocated an approach based on evidence, in which one makes claims and assumptions, and then one uses an architecture, arguments, and evidence obtained using formal method tools to build assurance.

He also presented a system architecture in which a Learning/Monitoring module checks assurance constraints and diagnoses failures. The assurance model module contains the parametric system model employed in the assurance case.

Cristoph Torens (DLR German Aerospace Center)

Cristoph Torrens presented an approach to get certification credit for an autonomous aircraft based on formal reasoning. The aircraft (RPAS) is a 15 kg rotorcraft, for which 3-D obstacles are mapped into a 3-D representation. The goal of his research is to answer the following questions: (1) How do we get RPAS certified? (2) How can autonomous behavior be modeled? (3) What degree of autonomy is needed? and (4) How can we have affordable certification credit for RPAS? His approach is based on formal methods.

System Requirements/Formal requirements have a huge impact on the certification of a system: Half of the certification safety objectives concern system requirements, and how they are met (means of compliance). Requirements can be properly formalized and matched with general GN&C systems. The requirements elicitation process is done with templates (based on LTL formulae) to obtain semi-formal requirements. These templates are designed for engineers not familiar with requirements management. The objective is to ensure that each low level requirement can be verified. The formalization is currently done manually, but the use of templates facilitates this task.

Offline and online runtime monitoring is also supported by his approach. Runtime monitoring is scalable, and represents low-hanging fruit in terms of effort, when working with formalized requirements. They use runtime monitoring to check traces of the system. For example, one can implement a runtime monitor for geo-fencing. This is useful for autonomy, for certification purposes. Cristoph Torrens claims that we do not have to care if the system is autonomous or not, because the implementation of the flight system is unimportant.

Darren Cofer (Rockwell Collins)

Darren Cofer presented a pragmatic approach for certifying autonomous systems based on existing standards (ARP 4761, 4754A, DO-297, DO 254, DO-178C). We already have DO-333 for getting certification credit on traditional systems. However, autonomous systems have new functionality based on adaptive and intelligent algorithms. As for the question of non-determinism often cited for autonomous systems, it usually comes from concurrency (multi-threaded computation in which execution impacts the result), uncertain existence of solutions, probabilistic algorithms, or environmental non-determinism.

For the most important and challenging aspects of certification, Darren Cofer listed: (1) well-defined requirements, (2) verifiable behavior, (3) predictable performance, (4) absence of unintended functionality, (5) complete assessment of behavior, (6) structural coverage metrics on code, and (7) transparent design.

For autonomous systems, Darren Cofer advocates the following mitigation strategies:

- Education (expertise gap between industry and regulators);
- Modified Certification Standards (new technology supplements), e.g., create supplement for adaptive algorithms;
- Alternative Certification Methods (assurance cases);

- New Verification Approaches (based on formal methods, probabilistic techniques etc.);
- Architectural Mitigation: bounded behavior of autonomy function, (e.g., considering a simplex controller vs. Adaptive function) engaged to recover aircraft during loss of surfaces, which could only be enacted during abnormal catastrophic conditions
- Licensing vs. Certification Paradigm Shift: we trust human operators because of training, operating experience, demonstrated performance in normal and emergency conditions, and an exam by licensing authority.

Darren Cofer concluded by presenting a certification challenge: if we have an autonomy algorithm that provides significant benefit can we answer the following questions: (1) Is the algorithm dependable? and (2) Can we produce arguments based on evidence that the algorithm is dependable?

Irene Gregory (NASA Langley)

Irene Gregory presented a different view of the problem. She comes from a controls background, rather than being an expert in formal methods. She actually still sees a lot of shortcomings in formal methods, and therefore, advocates the use of methods based on the evaluation of performance of control systems. She calls for the practical application of this philosophical approach in categories based on risk and innovation. As with the previous speakers, she is a proponent of bounding the behavior of autonomous systems where one only bounds unallowable behavior. She also made the statement that formal methods should take stochastic methods more into account.

6.2 Lightning fast talks

Robert Moore (Embry Riddle) presented a proposed set of rule changes that would allow model aircraft pilots of very small UASs (less than 5 lbs.) to fly autonomously, including beyond line-of-sight. This was based on his experience with flying such UASs recreationally.

7 Wrap-up session and Conclusions

The wrap up session focused on the future of the workshop. Many participants wanted to see the workshop continue, but we discussed what venue should be picked to associate the workshop with so that we ensure the right audience. In particular, there was a desire to involve regulators in the discussion. We also discussed how to avoid repeating issues that keep being discussed in such venues and how to be more focused towards solutions. For this reason, it was suggested that we select a topic and explore it in detail, and also that we define a challenge problem that participants can try to tackle. NASA Armstrong volunteered to provide a challenge problem based on their Expandable Variable Autonomy Architecture (EVAA).

Appendix A

List of Speakers

Session 1:

- Danette Allen (NASA Langley)
- Ella Atkins (University of Michigan)
- Andrew Lacher (MITRE)
- Lael Rudd (Lockheed Martin Advanced Technology Laboratories)
- Andy Thurling (AeroVironment)
- Fast talks:
  - Devesh Bhatt (Honeywell Aerospace Labs)
  - Corey Ippolito (NASA Ames research Center)
  - Greg Dorais (NASA Ames research Center)
  - Tom Apker (Naval Research Laboratory)
  - Yu Gu (West Virginia University)
  - Florian Adolf (DLR: German Aerospace Center)

Session2:

- John Valasek (Texas A&M University)
- Eric Johnson (Georgia Tech)

Session 3:

- Steve Young (NASA Langley)
- Kerianne Gross (AFRL),
- Jim Murphy (NASA Ames),
- Natalia Alexandrov (NASA Langley),
- Mats Heimdahl (University of Minnesota)
- Fast talks:
  - Mark Skoog (NASA Armstrong)
  - Jeorg Dittrich (DLR)

Session 4:

- Lee Pike (Galois)
- Natarajan Shankar (SRI)
- Cristoph Torens (DLR German Aerospace Center)
- Darren Cofer (Rockwell Collins)
- Irene Gregory (NASA Langley)
- Fast talks:
  - Robert Moore (Embry Riddle)

Appendix B

List of Participants

Florian Adolf (DLR)
Natalia Alexandrov (NASA Langley)
Danette Allen (NASA Langley)
Damodar Ambur (NASA Langley)
Manjula Ambur (NASA Langley)
Tom Apker (NRL)
Bimal Aponso (NASA Ames)
Omar Ariff (University of Salford)
Frank Arthurs (Texas A&M University)
Ella Atkins (University of Michigan)
Randall Bailey (NASA Langley)
Mary Baker (ATA Engineering)
Subodh Bhandari (Cal Poly Pomona)
Leandro Barajas (Dynetics)
Alec Bateman (Barron Associates)
Devesh Bhatt (Honeywell)
Stephen Blanchette (SEI)
Jovan Boskovic (Scientific Systems Company, Inc.)
Stuart Bowman (MITRE)
Guillaume Brat (NASA Ames)
David Bridges (Texas A&M University, Corpus Christi)
Clark Briggs (ATA Engineering, Inc.)
Neil Cameron (University of Liverpool)
Hai Yang Chao (University of Kansas)
Darren Cofer (Rockwell Collins)
Joerg Dittrich (DLR)
Ben DiVito (NASA Langley)
Greg Dorais (NASA Ames)
Val Evans (Lockheed Martin)
Doug Famularo (Texas A&M University)
Lisa Fern (San Jose State University)
Walter Fichter
Neha Gandhi (Barron Associates)
Starr Ginn (NASA Armstrong)
Kari Gonter (Metis Technology Solutions)
Dana Gould (NASA Langley)
Michael Gros (University of Stuttgart, Germany)
Kerianne Gross (AFRL)
Yu Gu (West Virginia University)
Craig Hange (NASA Ames)
Mats Heimdahl (University of Minnesota)

Jim Henrickson (Texas A&M University)
Keith Hoffler (Adaptive Aerospace Group, Inc.)
Corey Ippolito (NASA Ames)
Nidal Jodeh (AFRL)
Eric Johnson (Georgia Tech)
Gregory Kravit (Northrup Grumman)
Paul Kubiatko (Boeing)
Chetan S. Kulkarni (NASA Ames)
Andrew Lacher (MITRE)
Josh Love (Northrup Grumman)
Lin Ma (Zhejiang University, China)
Natesh Manikoth (FAA)
David Maroney (MITRE)
Catherine McGhan (Cal Tech)
Zohaib Mian (United Technologies Research Center)
Mark Milam (Northrup Grumman)
Robert Moore (Embry Riddle)
Terry Morris (NASA Langley)
Jim Murphy (NASA Ames)
Patrick Murphy (NASA Langley)
Takaya Otsuki (Georgia Tech)
Russ Paielli (NASA Ames)
Lee Pike (Galois)
Sangeeth Ponnusamy (Airbus)
Awais Raza
Nathan Richards (Barron Associates)
Jack Ryan (NASA Armstrong)
Lael Rudd (Lockheed Martin)
Dipanjan Saha
Pankaj Saini (University of Toronto, Canada)
Natarajan Shankar (SRI)
Kim Shish (Millenium Engineering & Integration Company)
Mark Skoog (NASA Armstrong)
Steven Snyder (University of Illinois at Urbana-Champaign)
Vahram Stepanyan (UC Santa Cruz)
Larry Strader (Jacobs Technology)
Chris Teubert (NASA Ames)
Chris Thames (NASA Langley)
Andy Thurling (AeroVironment)
Christoph Torens (DLR)
Ankit Tyagi (Intelligent Automation, Inc.)
Maartin Ujit de Harg (Ohio University)
Scott West (NASA Johnson)
Gregg Wildes (DornerWorks)
Shu-Chieh Wu (NASA Ames)
Steven Young (NASA Langley)

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704–0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01-05-2016	Technical Memorandum	

4. TITLE AND SUBTITLE
Workshop on Assurance for Autonomous Systems for Aviation

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Guillaume Brat, Misty Davies, Dimitra Giannakopoulou, Natasha Neogi

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
NASA Ames Research Center
Moffett Field, California 94035

8. PERFORMING ORGANIZATION REPORT NUMBER
L–

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSOR/MONITOR'S ACRONYM(S)
NASA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
NASA/TM–2016–219446

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified-Unlimited
Subject Category
Availability: NASA STI Program (757) 864-9658

13. SUPPLEMENTARY NOTES
An electronic version can be found at http://ntrs.nasa.gov.

14. ABSTRACT

This report describes the workshop on Assurance for Autonomous Systems for Aviation that was held in January 2016 in conjunction with the SciTech 2016 conference held in San Diego, CA. The workshop explored issues related to assurance for autonomous systems and also the idea of trust in these systems. Specifically, we focused on discussing current practices for assurance of autonomy, identifying barriers specific to autonomy as related to assurance as well as operational scenarios demonstrating the need to address the barriers. Furthermore, attention was given to identifying verification techniques that may be applicable to autonomy, as well as discussing new research directions needed to address barriers, thereby involving potential shifts in current practices.

15. SUBJECT TERMS
Autonomy, Assurance, V&V

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			STI Information Desk (help@sti.nasa.gov)
U	U	U	UU		19b. TELEPHONE NUMBER *(Include area code)* (757) 864-9658